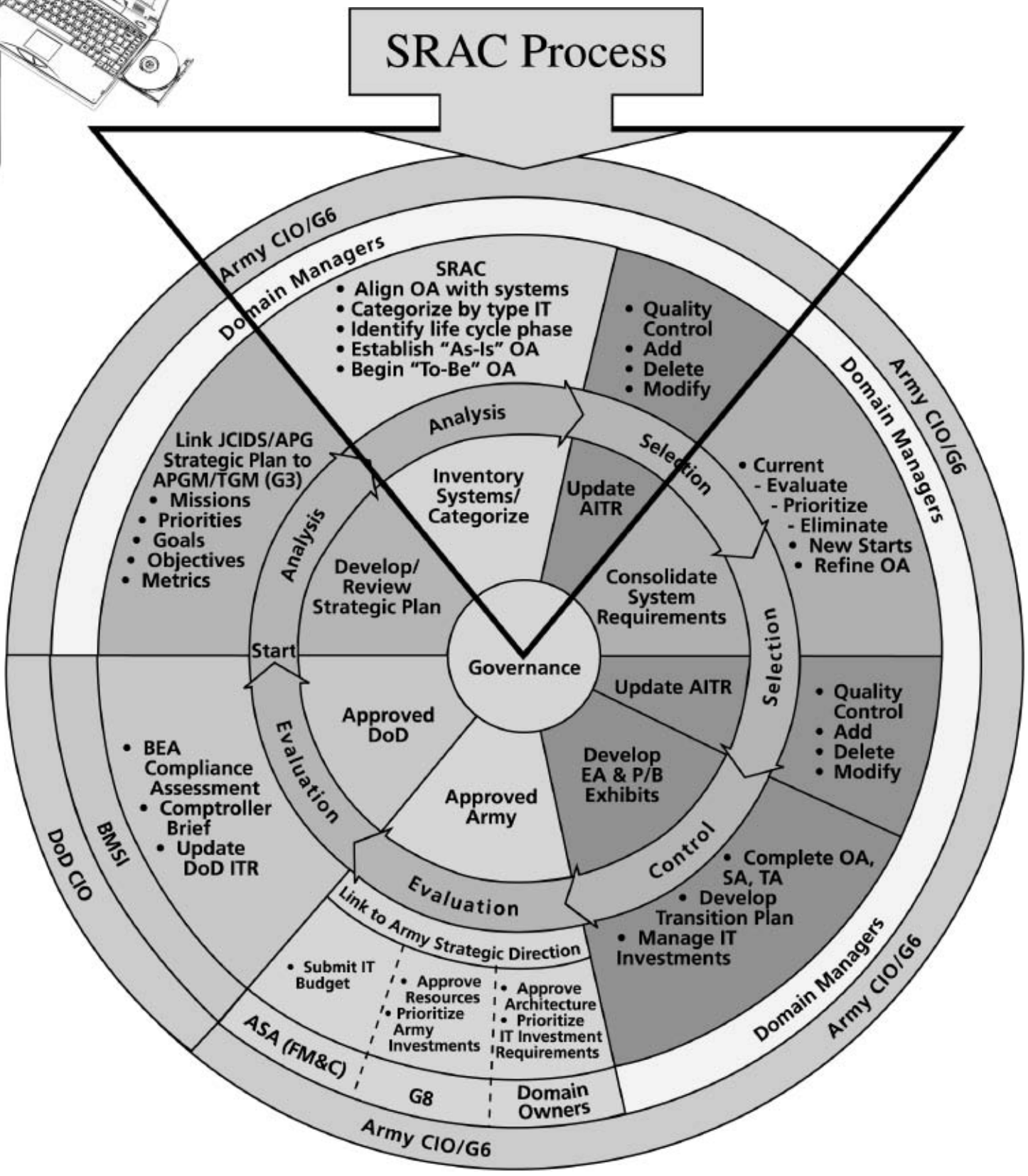
Army Systems Realignment And Categorization (SRAC) Guide

2nd Edition

July 2005

The Army Portfolio Management Process



MESSAGE

4 July 2005

Dear Reader,

Since the publication of the first Systems Realignment and Categorization (SRAC) guide, the Financial Management core business mission (CBM) area has completed their SRAC and is using the results to make decisions regarding which Information Technology (IT) Systems will remain in their IT portfolio.

As noted before, this SRAC Guide is to assist you with conducting a 100 percent IT systems inventory and categorizing your systems so you can identify the "As-Is" portfolio for your CBM area. This guide has been updated to reflect the Joint Capabilities Integration Development System (JCIDS) requirements for the development and funding of all new IT systems.

This guide walks you through the steps of the SRAC process using a proven methodology that allows you to identify what systems perform which functions in the current environment. The document follows the development of a web-based datacall, analysis of the results, and preparation of the final report.

Once your "As-Is" portfolio is identified, each CBM area will be able to move on to the next step in portfolio management (PfM)—consolidation of system requirements—where the CBM area will evaluate their current systems and prioritize them according to the benefit they bring to the Army. The CBM area will also review recommendations for new systems during this phase. New systems must support or modernize a strategic or operational requirement or capability that is not currently being supported, and it must align with the Army and the CBM area's Strategic Plan and the DoD net-centric environment.

By completing a full inventory of your business IT systems, you will have accomplished a key milestone that supports the DoD guidance on IT portfolio management. In turn, your efforts will support the Army's alignment to the Business Enterprise Architecture (BEA) and the Secretary of Defense's, Business Management Modernization Program (BMMP), which controls systems investments.

I am confident this Systems Realignment and Categorization Guide will be a valuable resource in your efforts to develop your "As-Is" IT portfolio and operational architecture. I encourage you to use this guide to complete this extremely important task.

Carla A. von Bernewitz

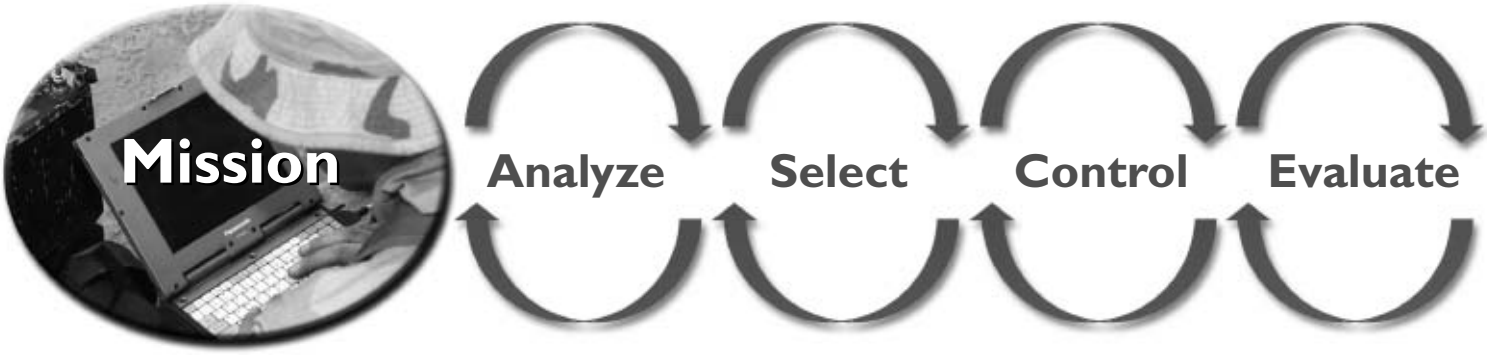
Director, AEIOO

ARMY SYSTEMS REALIGNMENT AND CATEGORIZATION PROCEDURES

The Joint Capabilities Integration and Development System (JCIDS); the Defense Acquisition System; and the Planning, Programming, Budgeting, and Execution (PPBE) process are DoD's three principal decision support processes for transforming the military forces.

JCIDS implements a capabilities-based approach that leverages the expertise of all government agencies, industry, and academia to identify improvements to existing capabilities and to develop new warfighting capabilities. This approach requires a collaborative process during the Functional Solution Analysis process that uses joint concepts and integrated architectures to identify capability gaps and redundancies. JCIDS examines where we are, where we want to be, what risks we face and what the potential costs are.

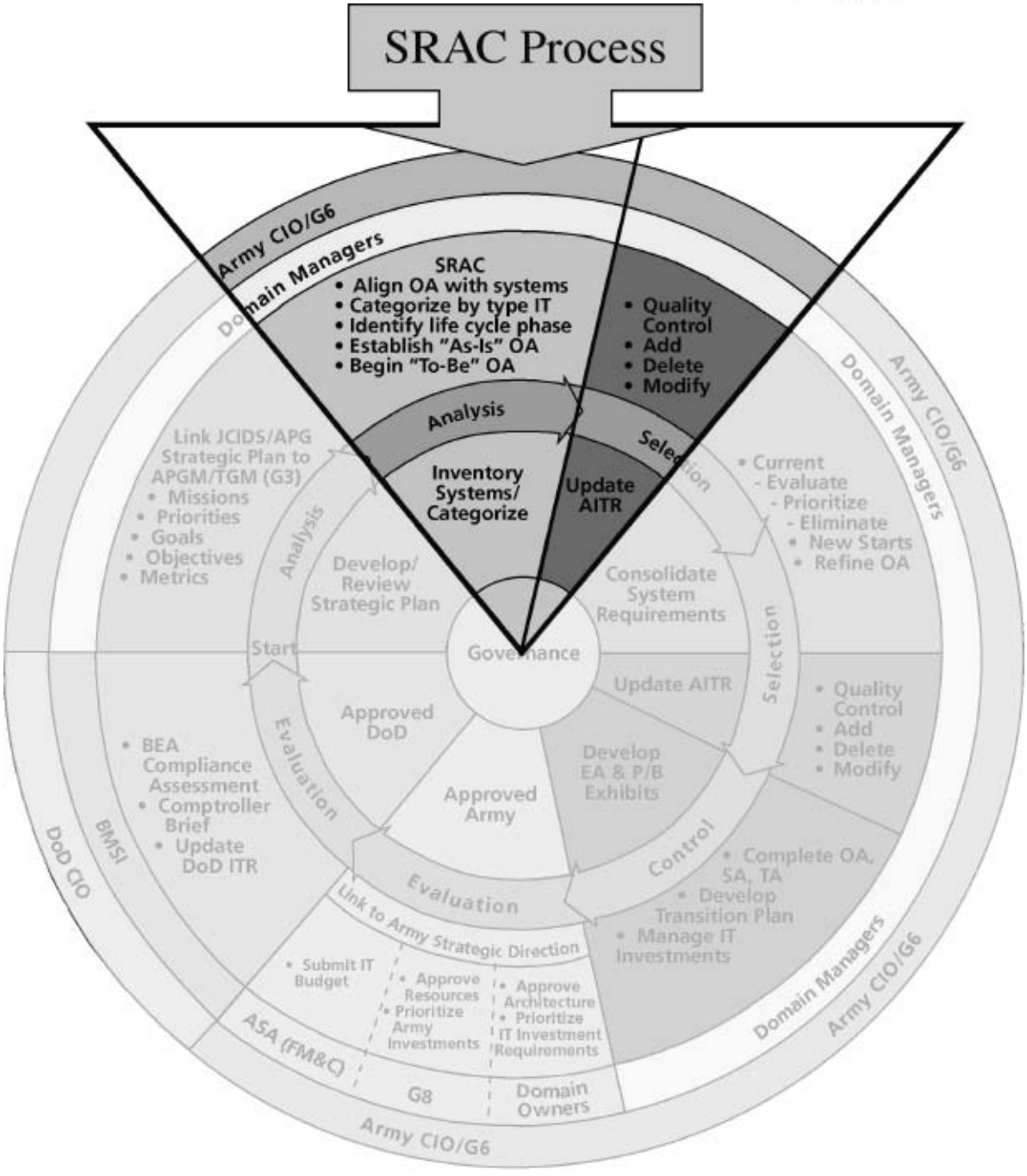
DoD's **directive**[1] on Information Technology (IT) Portfolio Management (PfM) assigns responsibilities for managing IT investments and states that IT investments shall be managed as portfolios. Specifically it states: "decisions on what IT investments to make, modify or terminate shall be based on the Global Information Grid (GIG) Integrated Architectures, core business mission (CBM) area goals, risk tolerance levels, potential returns, outcome goals and performance." The policy mandates that a portfolio management process will be established and are comprised of four core activities: analyze, select, control, and evaluate.



IT portfolios are important to the Army because they support warfighter/business requirements and can assist with the data requirements supporting the JCIDS analysis process. The results of the SRAC process provides valuable data on functional requirements, current information technology, and system investments.

[1] *Office of the Secretary of Defense, Information Technology Portfolio Management, 22 March 2004 (Enclosed)*

Within the Army, the Army CIO/G6 is responsible for portfolio management. Army portfolio management is a six-step process that mirrors DoD's four core PfM activities; analyze, select, control and evaluate.
(See Figure PfM Process below):



The six-step PfM process is as follows:

1. Review and develop the CBM area strategic plan, which is based on the results of the JCIDS functional solution analysis, the Army Plan (TAP); the Army Strategic Planning Guidance, the Army Planning Guidance (APG), and the Army Programming Guidance Memorandum (APGM), as well as the Army Campaign Plan.
2. Inventory and categorize systems and then update the Army Information Technology Registry (AITR).
3. Consolidate system requirements and then update the AITR.
4. Develop enterprise architecture (EA) and planning and budgeting exhibits.
5. Obtain Army approval—CBM area owner, CIO/G6, G8, and ASA (FM&C).
6. Obtain DoD approval—CBM area owner, Business Enterprise Architecture (BEA) Compliance Assessment, Defense Business Systems Modernization Committee (DBSMC), Department of Defense, Chief Information Officer (DoD CIO), and the Deputy Under Secretary of Defense, Acquisition, Logistics and Technology (DUSD, AT&L).

This document focuses on the second step in the IT portfolio management process: inventory and categorize systems and update the AITR. The SRAC Guide was developed to help inventory and categorize business mission area systems. The SRAC uses a web-based automated tool to collect and categorize data. It also provides a standard methodology for the collection and categorization of IT systems for each CBM area's portfolio—an important part of building and managing the portfolio.

The SRAC procedure is tailored by each CBM area to meet its specific mission area requirements, with the end state being a categorized list of IT assets. The results document a system's functionality, which provides the data required for the next step in the portfolio management process: consolidate system requirements. In this next step, the SRAC results can be used when making key decisions about which systems will remain in the CBM area's portfolio.

This SRAC guide describes the process of how to inventory and categorize the IT systems within a CBM area in order to make decisions about which systems should be retained, upgraded, or retired within the portfolio of systems. Before CBM area owners can inventory their systems, they must have, or develop a work breakdown structure (WBS), which will help them understand the functions and tasks supported by their systems. *More information regarding WBS can be found in Appendix A.*

In addition, data collected during the SRAC process can be used as a starting point to develop the operational views (OV), system views (SV), and technical views (TV) using the Department of Defense Architecture Framework (DODAF)[1] or other architecture tool that will represent the

[1] *The URL for the Department of Defense Architecture Framework (DODAF) is http://www.defenselink.mil/nii/doc/*

Phases. *The five guide phases*

future Army Enterprise Architecture. The data can also be used to update the AITR and the initial operational view activity model (OV-5) under the DODAF.

This guide—like the SRAC process—is divided into the five phases that ensure the Army's universe of systems is carefully inventoried and analyzed.

I. Conduct research and initial preparation

II. Develop the datacall

III. Conduct the datacall

IV. Categorize and analyze datacall results

V. Prepare final report

The figure below provides a crosswalk between DoD's four core activities, the Army's six phase Portfolio Management process, and the five phase SRAC process.

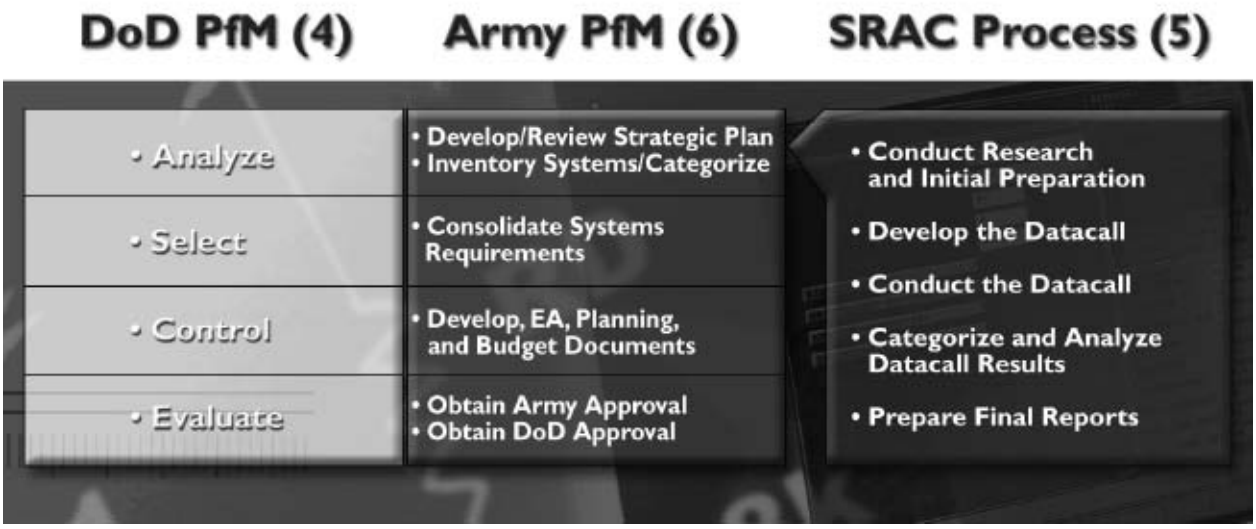
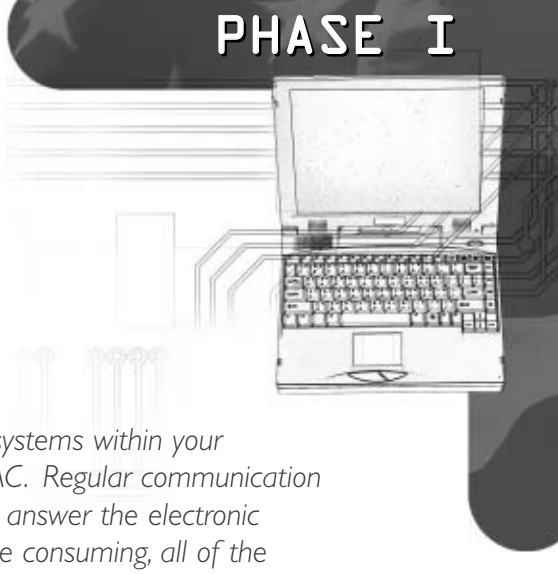


Figure 1. *Crosswalk of DoD Core Activities to Army Portfolio Management Process and SRAC Phases*

TABLE OF CONTENTS



PHASE I

CONDUCT RESEARCH AND INITIAL PREPARATION

This phase will give you the tools you need to successfully categorize the systems within your core business mission (CBM) area. It is the most critical phase of the SRAC. Regular communication between the Army's representative and the units or organizations that will answer the electronic datacall is imperative. Although the steps in this phase are often very time consuming, all of the requirements are necessary to successfully complete the datacall and the SRAC process.

At the onset, **identify the critical goals and objectives** for the electronic datacall based on the needs of the CBM area and the Army. The SRAC team, those who administer the SRAC process, should have a clear understanding of the data that needs to be collected to support the goals and objectives of the CBM, and to support the Army and JCIDS processes. By staying focused on these requirements, the questions asked during the electronic datacall can be limited to those that are necessary. This is important for minimizing the time it takes to complete the datacall and for maximizing the datacall participation rate.

Based on the goals and objectives, the CBM area should use standard DoD and Army definitions based on regulatory guidance for the IT information collected. These standard definitions should be annotated in the web-based datacall program.

Identify the key stakeholders for the SRAC project. This team must be capable of managing the project, tracking the timeline, developing the datacall questions, and analyzing and reporting the results. The team will also need a qualified software program analyst capable of developing or selecting a web-based datacall tool.

There are several administrative tasks that must be accomplished to successfully complete the SRAC. At the onset of Phase I, **collect point of contact information** from targeted organizations. The CBM area lead should sign a letter announcing the datacall and ask for appropriate POCs. This is a time-consuming action, as it takes time to staff and distribute the letter, and receive responses. This process can take as little as 35 days, but may take much longer unless it is managed carefully.

Once the goals and objectives have been defined, the team should obtain, if available, a functional work breakdown structure (WBS). If there is no WBS available, then one will have to be built. The functional WBS is the high-level description of the functional requirements that the CBM area systems support. Many CBM areas may be in the process of reengineering their business processes and developing functional WBS's; nonetheless, it is important to map current systems to a functional WBS that mirrors the functions that the current systems support.

The naming conventions for the first three functional levels should be functions, sub-functions, and supporting tasks. The function is the high-level task or CBM area (e.g., Financial Management). The sub-functions equate to the missions that support the major function (e.g., general ledger, accounts payable), and the supporting tasks are more specific tasks that support the sub-functions (update general ledger, record journal entries, etc.). *(See Figure 2).*

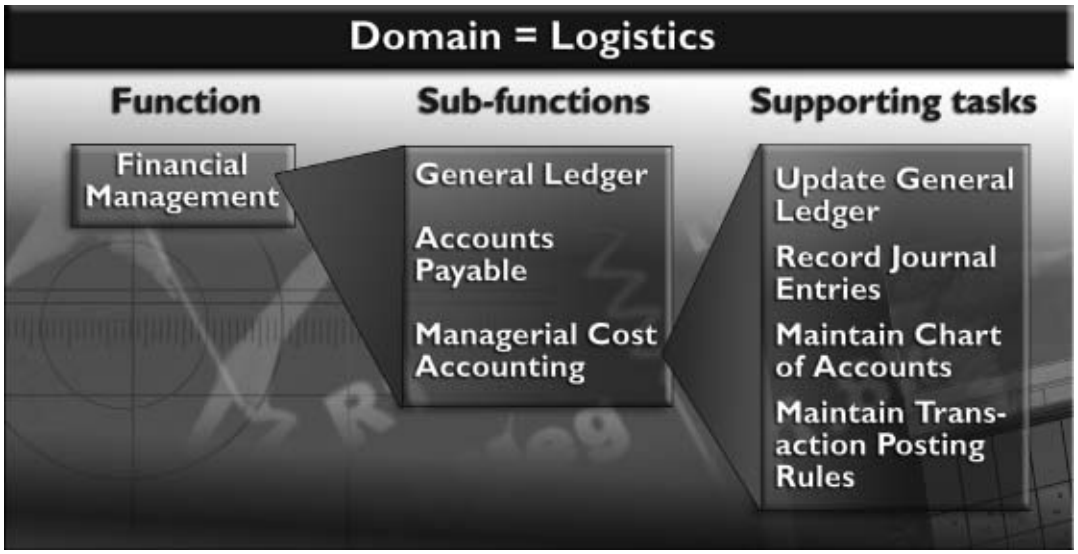


Figure 2. *Naming Conventions*

The CBM areas should move toward a standard reference model to document the WBS. DoD has recently released a draft set of enterprise architecture reference models (including a Business Reference Model [BRM]) that are specific to DoD functions. The naming conventions of these reference models should be used.

Identify target points of contact, those who will answer the datacall. First, it is important to know which organization you will target to answer the datacall. Second, identify who within these organizations should answer the datacall. Third, gather point of contact (POC) information on these organizations and people so you can communicate with these contacts in the future. Examples of organizations to target might include major commands (MACOMs), field operating agencies (FOAs), program executive offices (PEOs),

Domain	Sample Organization	Directorate	Division
Financial Management	TRADOC	G8	Finance and Accounting
Logistics	FORSCOM	G4	Logistics

Figure 3. *Identifying who should answer the datacall*

and Headquarters, Department of the Army (HQDA) staff. Who within the organization should answer the datacall depends upon what kind of information you are gathering. For example, if you are from the Financial Management CBM area, you should target the accountants or budget analysts *(See Figure 3)*.

Develop the datacall baseline. To do so will require the collection of databases from a variety of authoritative sources (i.e., AITR, DoD Information Technology Registry (DoD ITR), and Information Technology Management Application (ITMA)). The CBM area subject matter experts (SMEs) should review the baseline for redundancy and accuracy. The baseline must contain an organization responsible for each system for validation. Once refined, the baseline will be used to populate the datacall with known systems.

After all of these steps are complete, you are ready to begin Phase II and develop the datacall.

PHASE II
DEVELOP THE DATACALL

In this phase you complete a series of administrative tasks, outline the datacall requirements, develop a series of appropriate datacall questions, and program and test the datacall. At the close of Phase II you will be ready to implement a web-based datacall.

In Phase II, you will develop the questions for the datacall. Questions should be based on the key goals and objectives identified in Phase I, and if these questions are in the AITR/DoD ITR, the answers on the datacall should map appropriately to these sources. If the system supports a higher level requirement or process, i.e. JCIDS, the SRAC process is a good vehicle to collect required information.

How you organize and phrase questions is as important as the questions you ask. Their order and phrasing should be logical and easy to follow. There should be five key sections in the datacall: POC information, update/edit systems on the baseline, add systems to the baseline, budget, and comments. Additional sections can be added based on the core business mission (CBM) area's requirements.

There is flexibility in how the datacall is set up, so **collaboration with the datacall programmer or program analyst** is helpful when making development decisions. For example, who will answer the datacall, and how many levels will be built into the datacall, i.e. organization POC, secondary users, and tertiary users? The programmer can assign each MACOM a primary account to answer initial parts, and then set up analyst accounts so subordinate units can respond to latter parts. Another decision involves the authorization process. If a subordinate unit is answering the datacall, does the MACOM representative need to validate the entries? Should the MACOM have oversight of the data or the completion requirements?

These are just a few of the many questions that need to be asked, with answers provided to the programmer/program analyst in order to place the appropriate controls on the datacall.

Security requirements are another important consideration. Determine how screen names and passwords will be assigned and distributed, and what levels of control are necessary. Participants often forget passwords.

The programmer can develop a help utility to assist in resetting these passwords. The programmer can assist in setting up a help desk to facilitate communication between participants and the SRAC help desk team. There are a number of ways to facilitate help during the datacall. The easiest is to have the programmer develop a utility that sends an e-mail directly the help desk. The help desk should be able to answer both functional and technical questions.

While you are developing the questions for the datacall, additional administrative requirements need to be addressed. First you **determine how you will monitor the progress of the datacall.** It is important to identify who has completed the datacall, who has partially completed the datacall, and who has not started the datacall. Having an automated tool with real time information on the status of the datacall serves the government lead very well.

Next, you should **develop reminder letters** to send to participants who have not completed the datacall by set dates. Reminder form letters or e-mails should be sent at regular, programmed intervals throughout the datacall (e.g., halfway and three quarters of the way through) and should relay the number of working days remaining to meet the suspense date. Send out final notifications no later than 48 hours before the suspense date, remembering POC's are working in different time zones around the world. Based on participation rates toward the end of the datacall, the CBM area manager should send a reminder letter to organizations who have not fully complied with the datacall requirement.

Finally, **identify how long you will keep the datacall open** (21 calendar days is recommended). Interaction with participants is essential to the success of the datacall and will preclude the need for an extension. In fact, failure to communicate with the non-responsive organizations will jeopardize the quality of the data received for final SRAC analysis.

Remember to test the datacall—and all supporting technology—to ensure it works. **Meet with the CBM area owner or representative** to demonstrate what they will be presenting to the Army.

Once the chain of command has viewed and approved the datacall it is time to conduct the datacall, which is Phase III.

PHASE III
CONDUCT THE DATACALL

During this phase you will conduct the actual web-based datacall for the length of time determined in Phase II. At the close of Phase III you will be ready to categorize and analyze the datacall results.

The first step in Phase III is to **initiate the datacall.** E-mail instructions for completing the datacall to each participant in order to initiate the datacall. Personalized instructions should include screen names and the website address, as well as the corresponding password.

Regularly **monitor the datacall** to check its completion status. Send out letters (at intervals determined in Phase II) to the commands that have not completed the datacall, reminding them of the number of working days remaining to meet the suspense date. Also, provide your chain of command with a weekly status report. The government point of contact should coordinate daily with the datacall participants via telephone. These frequent calls to participants can increase the SRAC participation level. Low levels of participation results in a lack of data, which can severely impact both the quality and the results of the datacall.

Staff the datacall help desk throughout the datacall, and ensure attendants can provide any technical and functional support according to fixed customer service standards. If time permits, you can start planning for Phase IV.

At the conclusion of the datacall, the participation results should be provided to the core business mission (CBM) area. If the results are not adequate, consider extending the datacall for a short period to capture the required information. Once you **close the datacall** and the CBM area manager is satisfied with the participation level, you are ready to categorize and analyze the data in Phase IV.

PHASE IV
CATEGORIZE AND ANALYZE DATACALL RESULTS

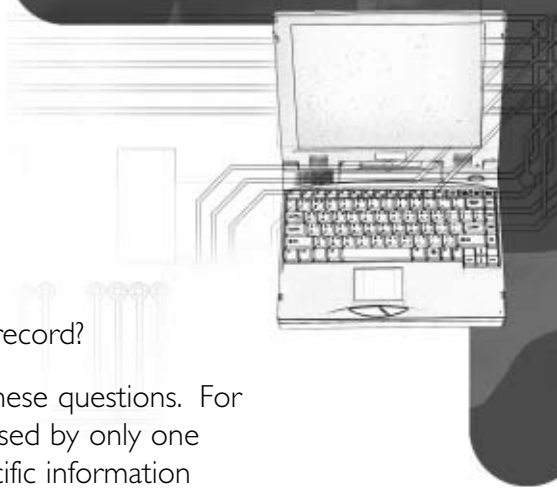
By the end of this phase, you will be ready to produce a final report. In Phase IV you will categorize and analyze the information collected during the datacall.

The first step in this phase is to **categorize your data** according to the types of systems you decided to collect in Phase I. For example, if you choose to examine only automated information systems (AIS), you need to examine the updated baseline and categorize the line items according to that type of IT. All other line items (databases, enabling technology, etc.) should be excluded from your final list before you analyze the data. There are a number of ways to categorize your data:

- Systems not reviewed
- Systems not validated
- Retired systems
- Non-Army systems
- Systems not relative to your core business mission (CBM)
- Non-systems

Once all the data entries have been categorized, **analyze the data** based on the type of IT and the system information you need. During analysis, you are looking for trends, issues, and key findings for your final report. The answers to the following questions are critical for completing a well thought out analysis of a CBM area:

- Which systems support which functional areas?
- Which systems belong to which CBM areas?
- Which systems are mission-critical or mission-essential?
- Which systems have what kind of technology?
- Which systems have interfaces?
- What kind of technology do the systems with interfaces employ?
- Which systems are unique to the MACOM or organization?
- Which systems are scheduled for consolidation or retirement?



- Which life cycle phase of the Defense Acquisition System does the system reside?
- Which systems require JCIDS review/approval?
- Which systems are registered in the Army and DoD database of record?

Review the datacall results and **identify trends** that might answer these questions. For example, if more than 50 percent of the systems and databases are used by only one MACOM or organization, it might be important to identify more specific information for MACOM or organization-unique systems:

- What are the names and descriptions of these unique systems?
- What organization owns the unique systems?
- What functions, sub-functions, and supporting tasks do these unique systems support?
- Are any of these unique systems scheduled for consolidation/retirement?
  - Which ones?
  - When will that occur?
  - What system, if any, will replace them?

Interfaces might be another area for further analysis. If a high number of interfaces are reported, identify additional information about them based on the data you collected. Consider the following questions:

- How many systems have interfaces that connect to systems that are scheduled for consolidation/retirement?
- How many unique systems have interfaces with systems scheduled for consolidation/retirement?
- How many systems with interfaces are mission-critical?
- Which mission-critical systems are unique and have interfaces?

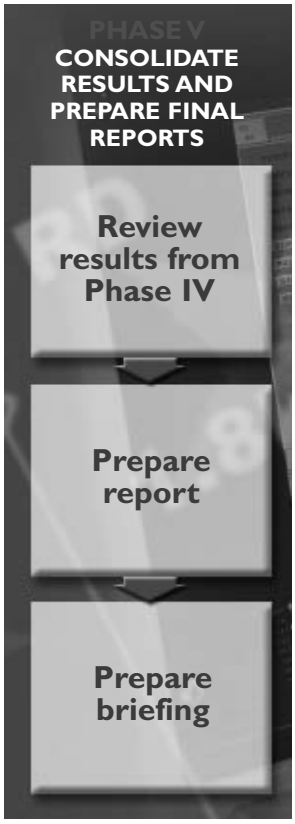
Review of this more defined data will **expose several key findings,** which you can examine further to illustrate your key points. These key points should be illustrated to clearly show your findings. You can show a number of different data fields on one illustration to make your point. For instance, you can identify supporting tasks and sub-functions to specific systems, show mission essentially, and indicate systems that should be scheduled for consolidation—all on one chart.

Once the results have been categorized and the analysis is complete, it is time to move to Phase V to consolidate the results and prepare the final report.

PHASE V
CONSOLIDATE RESULTS AND PREPARE FINAL REPORT

During this phase, you will review the information collected in Phase IV and start writing a final report.

Once you completely **review the results from Phase IV**, you are ready to **prepare your report.** The report can be written in many different formats. However, to get a good picture of the SRAC results, and to document the history of the datacall, consider breaking the report into the following three sections, using illustrations wherever applicable:



1. Datacall participation results
2. Datacall results based on statistics after categorization
3. Datacall findings based on the analysis of the data

DATACALL PARTICIPATION RESULTS

When reporting the datacall participation results, present participation statistics—namely how many participants answered the datacall and any significant information that might have contributed to low (or high) participation numbers. Charts can be very effective in displaying complex information across several different areas. This chart identifies which organizations were responsible for participating in the datacall, the number of systems the organization was responsible to answer, and the number of automated information systems (AISs) that were added during the datacall. *(See Figure 4)*.

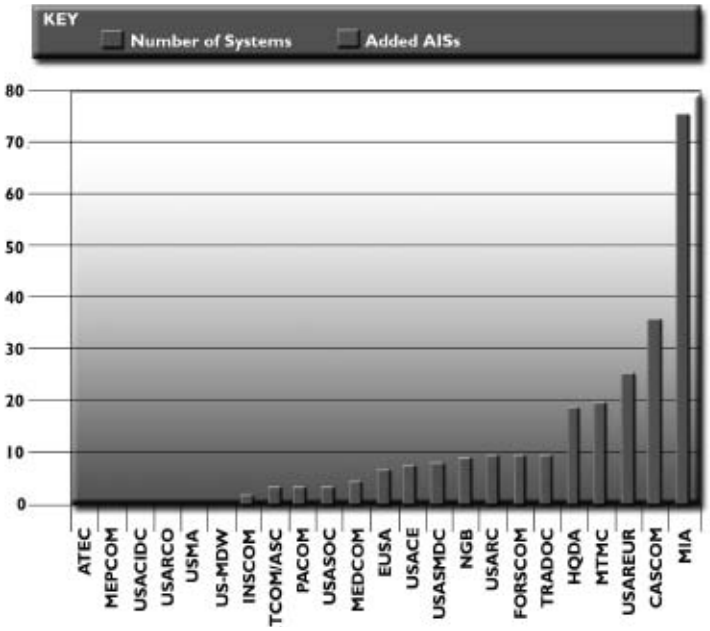
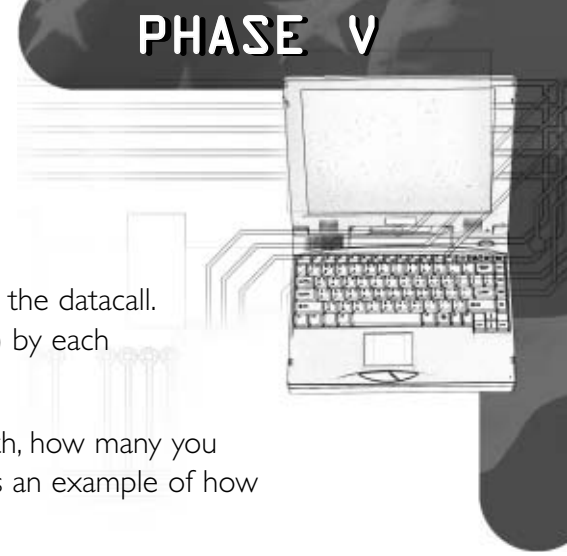


Figure 4. *Sample datacall Participation Chart*



DATACALL RESULTS

In the next section, present the systems information reported during the datacall. Review how many systems were reported (or added to the datacall) by each participant, and how many systems each participant updated.

This section should also convey how many line items you started with, how many you ended with, and how you got from one point to another. *Figure 5* is an example of how to best convey this information.

	Adjustment	Balance
+Consolidation		800
-Duplicates	(300)	500
-Non-AIS	(300)	200
+Datacall Results	150	350
-Databases	(50)	300
-Enabling Technology	(25)	275
-Other	(150)	12
-Duplicates	(20)	105
-Joint	(10)	95
-DoD	(10)	85
AIS		85

Figure 5. *Sample datacall Results Table*

DATACALL FINDINGS

The final portion is the most important part of the datacall. In it, you will summarize key findings, align the findings with the goals and objectives identified in Phase I, and then explain trends that were identified as a result of the analysis in Phase IV, using illustrations where appropriate.

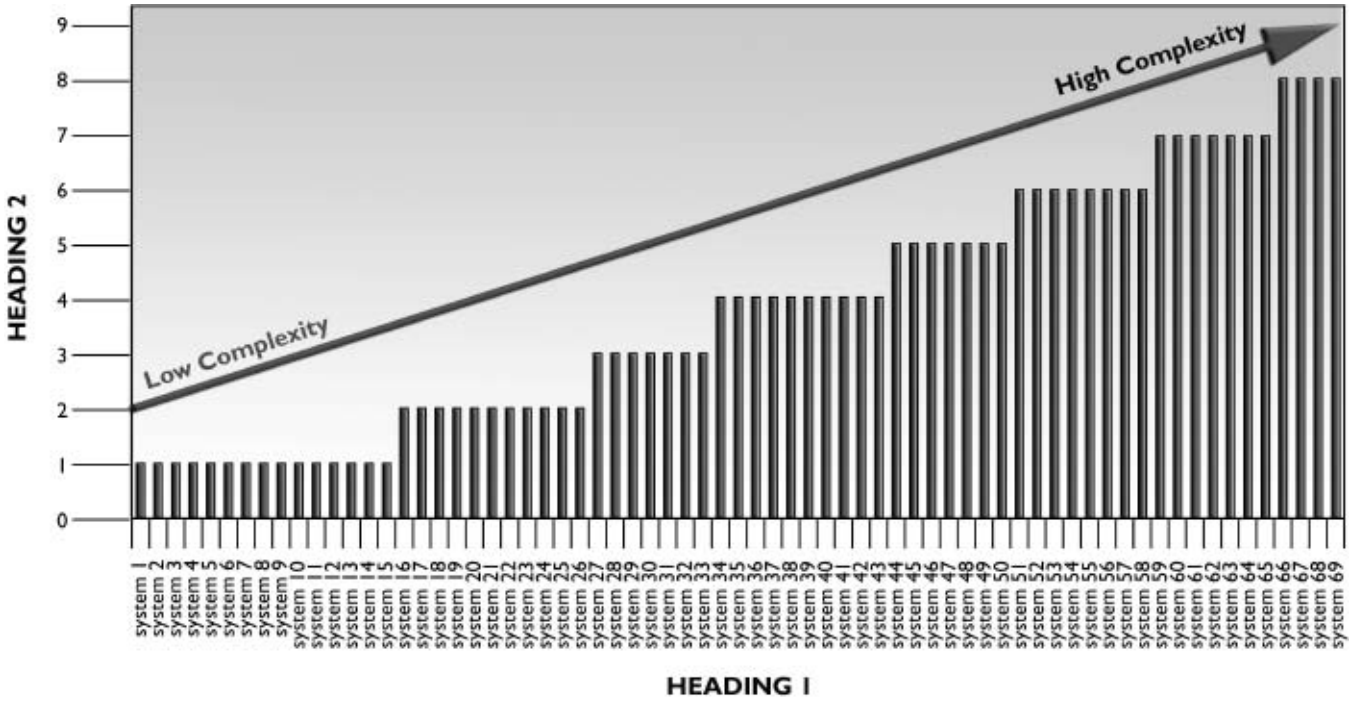
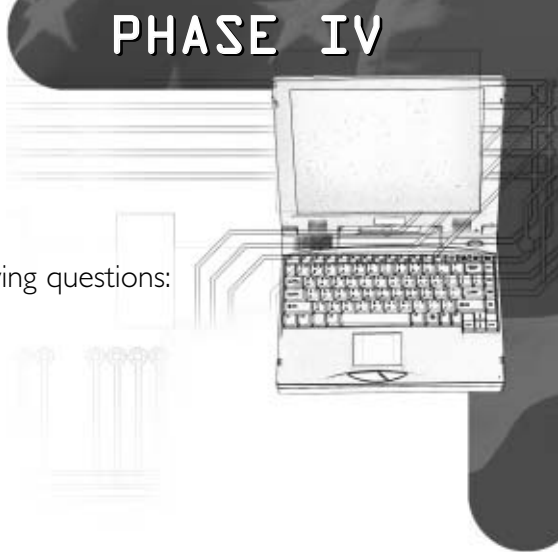


Figure 6. *Sample Illustration of datacall Findings*

Figure 6 is an example of how data can be displayed in the final report. This chart illustrates the complexity of system functionality. It shows the number of sub-functions or supporting tasks that each system supports and assigns a level of complexity. If you are going to eliminate a system, it is important to remember, the more functions a system supports, the more interfaces it may have, and the more complex it may be to eliminate. A system supporting only one sub-function may be easier to eliminate or consolidate than one with several sub-functions.



Other illustrations *(Figure 7)* can graphically answer many questions identified in Phase IV. For example, this illustration answers the following questions:

- Which systems support which sub-functions and supporting tasks?
- Which systems are mission-critical or mission-essential?
- Which systems are unique to the MACOM or organization?
- Which systems are scheduled for consolidation or retirement?

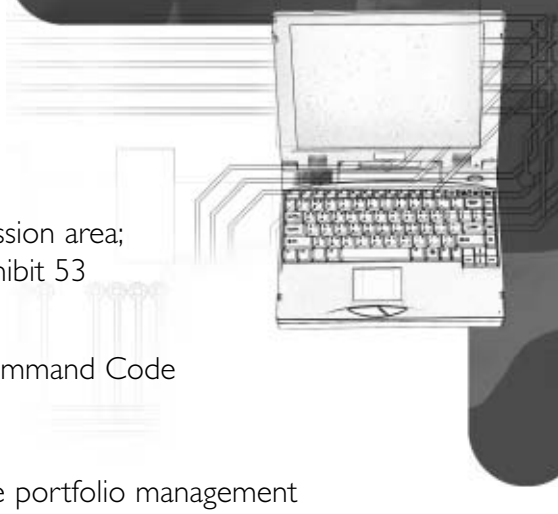
	Scheduled for Consolidation											Not Currently Scheduled for Consolidation																				
	Mission Critical	Mission Essential								Other		Mission Critical		Mission Essential																Other		
Sub-functions/Supporting Tasks	AORS	ATTCMIS	dbCAS	eSTADIS	ETS	FC/SSF	FEDS	FIRST	IMA-OnLine	AVKINPUT	CIMS	FMSS	FPU	RLAS	216DBR	ABIF	ACCPAC	AFCOS	APCS	ARMS	ASARS	AUDTRAIL	BIS	BRAC FM	CAB	CARE	CBS	CEEMIS	CEFMS	CMS2	AMDBES	ASK-FM	AWPS
5.0 General Ledger						X											U		U						X				U			
5.1 Maintain Chart of Accounts																	U		U										U			
5.2 Maintain Transaction Posting Rules																	U												U			
6.0 Property, Plant, and Equipment					U									U															U			
6.1 Maintain/Update Real Property Information					U									U															U			
6.2 Maintain/Update Personnel Property Info.					U																								U			
6.3 Maintain/Update Plant and Equipment Info					U									U															U			
7.0 Revenue and Accounts Receivable					U					X				U		U	U		U						X		U		U			
7.1 Recognize Revenue					U											U	U								X				U			
7.2 Establish Accounts Receivable					U					X							U		U						X		U		U			
8.0 Managerial Cost Accounting	U	U		U	U		U		U		U			U									U		X				U	U		U
8.1 Cost Management	U	U		U	U		U		U		U												U		X				U	U		
8.2 Cost Forecasting and Analysis					U				U																								U
9.0 Human Resources and Payroll	U		X													U		U											U			
9.1 Perform Personnel Processing	U																	U														
9.2 Collect Human Resource Data	U		X																										U			
9.3 Maintain Human Resource Data	U																	U														
10.0 Material Inventory Value			X		U														U										U			
10.1 Record Inventory Value					U																								U			
10.2 Record Inventory in Storage Value																			U										U			
11.0 Funds Control and Budgetary Accounting	U		X	U	U	X		U	U	X	U	X	U			U		U	U						X				U	U	X		
11.1 Record Budget Authority/Fund Allocation	U		X						U			X																	U		X		
11.2 Maintain Funds Availability	U		X		U	X		U	U			X				U		U											U	U	X		
11.3 Record Commitments	U		X		U			U	U		U					U		U											U		X		
12.0 Accounts Payable					U									U			U		U						X	X	U		U				
12.1 Maintain and Update Payee Information					U												U		U						X	X	U		U				
12.2 Recognize Liabilities/Establish Payables					U												U								X	X			U				

Figure 7. *Alignment of sample WBS systems along the mission critical spectrum*

CONCLUSION

In conclusion, the SRAC process can provide the core business mission (CBM) area manager with the information required to build and manage the IT portfolio as listed below:

- "As-Is" activity model required for the operational architecture of the CBM area (OV-5)
- "As-Is" operational to systems function traceability matrix for the CBM area (SV-5)
- Functional work breakdown structure for the mission area
- Inventory of systems with descriptions, with the supported tasks, and the level the systems are used and located
- Inventory of systems with functionality, mission essentially, and uniqueness
- Inventory of systems scheduled for consolidation and system replacement
- Inventory of systems by acquisition life cycle phase
- Inventory of systems based on primary, secondary, and tertiary functionality
- Complexity analysis by number of systems that support each sub-function
- Complexity analysis by number of systems that support each supporting task
- Inventory of systems by organization, sub-function, and supporting tasks
- Inventory of systems by mission essentially, organization, sub-function, and supporting tasks
- Inventory of systems by acquisition life cycle phase, organization, sub-function, and supporting tasks
- Interfaces with other IT systems
- Overview of unique systems based on which sub-function supported, by scheduled date of consolidation, with the identification of unique systems having interfaces
- Proponent points of contacts for systems scheduled caegorized as unique or scheduled for consolidation
- Consolidation schedule for systems by name, replacement date, and replacement system
- Technical profile for the CBM area portfolio
- Technical Data to include: Database engines, communications means, operating systems, programming language, system type, and types of IT services



- Inventory of systems by type IT and IT services provided
- Miscellaneous data on each system depending on needs of mission area; i.e. is it on the AITR, is it on the DoD ITR, does it have an exhibit 53 or exhibit 300?
- Budget data on systems by MDEP, appropriations, APE, and Command Code
- Investment profile for the CBM area portfolio

After the **SRAC process is complete,** the next step within the portfolio management process is to **update the AITR.** The CIO/G6 can facilitate the effort to transfer electronic data. The CBM area manager is responsible for the quality control of the CBM area's IT systems listed on the AITR, and will coordinate with the other Army CBM areas to resolve any conflicts in system ownership.

Once the data is updated on the AITR, the entire registry should be evaluated. If a system is not on the validated SRAC list, but is on the AITR, it should be scheduled for review in the Consolidation Phase.

Once the CBM area IT systems are added, deleted, or categorized based on the results of the SRAC process, you are ready to **consolidate systems requirements**—the next step in the portfolio management process.

This is the opportunity for the CBM areas to evaluate the current IT systems based on the SRAC output, and consider new starts. Systems will be evaluated, prioritized, and scheduled for disposal, as appropriate. New starts will be considered based on JCIDS capability requirements, Army systems requirements and CBM area approval. The results of the SRAC can be beneficial in the functional solution analysis and in developing the ICD, CDD, and CPD during the JCIDS process.

DEPUTY SECRETARY OF DEFENSE
1010 DEFENSE PENTAGON
WASHINGTON, DC 20301-1010

MAR 22 2004

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, PROGRAM ANALYSIS AND EVALUATION
DIRECTOR, NET ASSESSMENT
DIRECTOR, FORCE TRANSFORMATION
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Information Technology Portfolio Management

Attachment establishes DoD policies and assigns responsibilities for managing information technology (IT) investments as portfolios. Decisions on what IT investments to make, modify or terminate shall be based on architectures, risk tolerance levels, potential returns, outcome goals and performance. While the guidance specifically addresses IT portfolios and a process for making tradeoffs among IT projects, the IT portfolio is part of the Department's broader portfolio of investments. In this larger context, tradeoffs will have to be made between IT and non-IT investments in other agency processes.

This guidance applies to the six Joint Warfighting Capability Assessment areas (i.e., Battlespace Awareness, Command and Control, Force Application, Protection, Focused Logistics, and Net Centricity), the six Business Domains (i.e., Accounting and Finance, Acquisition, Human Resources Management, Installations and Environment, Logistics, and Strategic Planning and Budgeting), and the underlying Enterprise Information Environment. Improved and timely IT investment policies are a cornerstone to enable change throughout the Department, assure that we have the right IT capabilities to perform our mission and conduct effective information operations, eliminate outdated ways of doing business, and achieve our net-centricity goals. While the attached policy is effective immediately, to ensure that this policy is institutionalized, I ask that the DoD Chief Information Officer, in coordination with the Director, Administration and Management, incorporate it into the DoD Directive System within 180 days.

Paul Wolfowitz

Attachment:
As stated

OSD 03246-04

Department of Defense

ASD(NII)/DoD CIO

SUBJECT: Information Technology Portfolio Management

References: (a) Office of Management and Budget Circular No. A-130, "Management of Federal Information Resources," Revised, (Transmittal Memorandum No. 4), November 28, 2000
(b) DoD Directive 8000.1, "Management of DoD Information Resources and Information Technology," March 20, 2002
(c) DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002
(d) Chairman of the Joint Chiefs of Staff Instruction 3170.01, "Joint Capabilities Integration and Development System," June 24, 2003
(e) DoD Directive 5000.1, The Defense Acquisition System," May 12, 2003
(f) DoD Directive 4630.5, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), January 11, 2002

1. PURPOSE

This document:

1.1. Consistent with references (a) and (b) and (c), establishes policies and assigns responsibilities for the management of DoD information technology (IT) and associated investments as portfolios.

1.2. Provides fundamental concepts for managing a portfolio of IT investments that focus on improving business and warfighting outcomes and capabilities.

2. APPLICABILITY AND SCOPE

2.1. This document applies to:

2.1.1. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as "the DoD Components").

2.1.2. Joint Warfighting Capability Assessment areas, Business Domains, and the underlying Enterprise Information Environment.

2.1.3. All current and planned IT resources that enable the achievement of Enterprise outcome goals.

3. DEFINITIONS

Terms used in this document are defined in enclosure 1.

4. POLICY

It is DoD policy that:

4.1. Information technology (IT) investments shall be managed as portfolios. Decisions on what IT investments to make, modify or terminate shall be based on the Global Information Grid (GIG) Integrated Architecture, mission area goals, architectures, risk tolerance levels, potential returns, outcome goals and performance.

4.2. Portfolios shall be managed using integrated strategic planning, integrated architectures, measures of performance, risk management techniques, transition plans, and portfolio investments strategies.

4.3. Portfolio management processes shall be established and comprised of the following core activities:

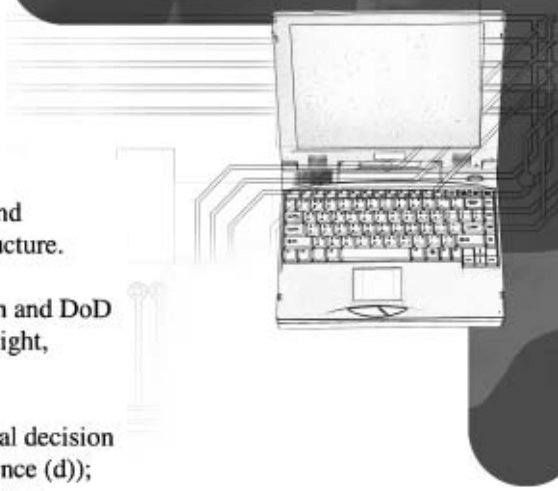
4.3.1. Analysis that links Mission Area goals to DoD Enterprise vision, goals, objectives, priorities, capabilities, as well as how these will be achieved and measured; identifies gaps and opportunities; identifies risks and how these will be mitigated; provides for continuous process improvement; and determines strategic direction for mission area activities and processes.

4.3.2. Selection that identifies the best mix of IT investments to achieve outcome goals and plans as well as transition to "to-be" architectures.

4.3.3. Control that ensures a portfolio and individual projects in the portfolio are acquired in accordance with cost, schedule, performance and risk baselines and documented technical criteria, and remain consistent with the current approved version of the GIG Integrated Architecture.

4.3.4. Evaluation that routinely and systematically assesses and measures actual contributions of the portfolio as well as supports adjustments to the mix of portfolio projects, as necessary.

4.4. Integrated Architectures with Enterprise-, Mission Area-, Domain and DoD Component-level perspectives shall be developed, maintained and applied to gain a better understanding of the organization, and the capability gaps between the current and future environments (warfighting and business); assess process improvement opportunities within and across the levels; determine



interoperability and capability requirements; promote standards; identify and implement information assurance requirements; formulate and target investments to improve data and information management; and identify the required capabilities of the technical infrastructure.

4.5. Portfolios shall be nested and integrated at the Enterprise, Mission Area, Domain and DoD Component levels and shall be based on the principles of centralized guidance and oversight, stakeholder participation, collaborative decision making, and decentralized execution.

4.6. Portfolio management processes shall leverage each of the Department's principal decision support systems (i.e., the Joint Capabilities Integration and Development System (reference (d)); Planning, Programming, Budgeting and Execution process; and Defense Acquisition System (reference (e)).

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Networks and Information Integration, as the DoD Chief Information Officer (DoD CIO), shall:

5.1.1. Establish a process for maximizing the value and assessing and managing the risks of DoD IT investments, consistent with this policy and reference (b).

5.1.2. In coordination with the OSD Principal Staff Assistants, and the Chairman of the Joint Chiefs of Staff, issue procedures for the policies contained herein. This shall include a core set of uniformly applied criteria for portfolio selection and evaluation.

5.1.3. Ensure that integrated architectures (warfighting and business), and their component parts, comply with the GIG Integrated Architecture (reference (c)).

5.1.4. Develop and maintain the DoD Information Resources Management Strategic Plan.

5.1.5. Provide for the enterprise information environment and ensure that its capabilities are synchronized with requirements for these capabilities. This shall include providing for a common set of Enterprise capabilities that enable users (consumers and providers) to discover, access, post, process, advertise, retrieve and fuse data, and make sense of data gathered.

5.1.6. Establish and co-chair, with other senior officials, executive-level governance forums that provide strategic direction, identify opportunities and resolve cross-functional issues that are in the best interest of the Enterprise.

5.2. The Under Secretary of Defense (Comptroller)/Chief Financial Officer shall:

5.2.1. Establish policies and procedures to ensure that accounting, financial and asset management, and other related DoD IT business systems are designed, developed, maintained, and

used effectively by the DoD Components to provide financial data reliably, consistently and expeditiously, and support programmatic IT investment decisions, consistent with this policy and reference (b).

5.2.2. In coordination with the DoD CIO and the Principal Staff Assistants, develop and maintain the DoD Business Enterprise Architecture (BEA) and associated Business Enterprise Transition Plan as a component of the GIG Integrated Architecture.

5.2.3. Identify and manage the resolution of cross-cutting issues, facilitate future BEA development, and review budgets and make recommendations to ensure that funds are budgeted to implement the portfolio of BEA projects.

5.2.4. Establish and co-chair, with the DoD CIO, executive-level governance forums that provide strategic direction, identify opportunities and resolve cross-functional issues affecting the business community.

5.3. The Under Secretary of Defense for Acquisition, Technology and Logistics shall ensure policies and procedures contained herein are effectively implemented, consistent with this policy and references (b) and (e).

5.4. The OSD Principal Staff Assistants shall, according to their responsibility and authority for assigned business areas:

5.4.1. Designate Business Domains, in coordination with the DoD CIO and the USD(C)/CFO, and ensure that the following tasks are executed consistent with business enterprise guidance and direction:

5.4.1.1. Establish a repeatable IT portfolio management process, including governance structure(s), consistent with the policies contained herein. This process shall include the core activities described in paragraph 4.3 above, and shall be communicated widely and cascaded down to the DoD Components so that they can understand expectations and effectively participate in the process.

5.4.1.2. Participate in business enterprise governance forums aimed at identifying opportunities for commonality in portfolio management techniques, and providing solutions to problems that are in the best interest of the Enterprise.

5.4.2. In coordination with the DoD CIO, issue policies and procedures that implement the policies contained herein.

5.5. The Director of Program Analysis and Evaluation shall review and issue programming and budgeting guidance that reflects (warfighting and business) portfolio recommendations to continue, modify, terminate or initiate funding for IT projects/programs to ensure compliance with the GIG Integrated Architecture and associated applications.

5.6. The Chairman of the Joint Chiefs of Staff shall:

5.6.1. Perform warfighting mission area control and oversight of supporting information systems, and ensure warfighting mission area leadership throughout the systems' life-cycle phases, consistent with this policy and reference (b).

5.6.2. In coordination with the DoD CIO, issue policies and procedures that implement the policies contained herein, and participate in warfighting enterprise governance forums aimed at identifying opportunities for commonality in portfolio management techniques and providing solutions to problems that are in the best interest of the Enterprise.

5.7. The Heads of the DoD Components shall, as appropriate, execute the tasks described in Paragraphs 5.4 and 5.6 above.

5.8. The DoD Component Chief Information Officers shall provide advice and other assistance to the Component Head and other Component senior management personnel to ensure that information resources are acquired, used, and managed by the DoD Component consistent with the policies contained herein.

6. EFFECTIVE DATE: This document is effective immediately.

E1. ENCLOSURE 1

DEFINITIONS

E1.1.1. Enterprise Information Environment: The common, integrated computing and communications environment of the Global Information Grid. The GIG EIE is composed of GIG assets that operate as or that assure local area networks, campus area networks, tactical networks, operational area networks, metropolitan area networks and wide area networks. The GIG EIE is also composed of GIG assets that operate as or that assure end user devices, work stations and servers that provide local, organizational, regional or global computing capabilities. The GIG EIE includes all software associated with the operation of EIE assets and the development environments and user productivity tools used in the GIG. The GIG EIE includes a common set of Enterprise and mission specific services, called GIG Enterprise Services, which provide awareness of, access to and delivery of information on the GIG.

E1.1.2. Global Information Grid Integrated Architecture. The DoD-wide enterprise architecture that depicts warfighting and business domains.

E1.1.3. Information Resources. Information and related resources, such as personnel, equipment, funds, and information technology.

E1.1.4. Information Resources Management. The process of managing information resources to accomplish Agency missions and improve Agency performance, including through the reduction of information collection burdens on the public.

E1.1.5. Information Technology. Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by the DoD Component. For purposes of the preceding sentence, equipment is used by a DoD Component if the equipment is used by the DoD Component directly or is used by a contractor under a contract with the DoD Component that (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. It also includes National Security Systems as defined in reference (b). Notwithstanding the above, the term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

E1.1.6. Integrated Architecture. An architecture consisting of multiple views or perspectives (operational view, system view, and technical view) that facilitates integration and promotes interoperability across Family-Of-Systems / System-of Systems and compatibility among related mission area architectures (ref (f)).

E1.1.7. Mission Area: A defined area of responsibility whose functions and processes contribute to accomplishment of the mission.

APPENDIX A
Building a Work Breakdown Structure (WBS) for SRAC

1. Definition:

A WBS is a consistent and visible framework for defense materiel items, information technology systems and contracts within a program.

2. Procedure

a. Consult: MIL-HDBK-881, DoD Handbook Work Breakdown Structure, 2 January 1998 (Revised version scheduled June 2005).

b. Research other examples of WBS that have been used with DoD and industry.

c. Build a WBS based on the tasks that are performed by the functional area.

d. Research current systems development literature to identify the functional WBS used to design the system. This is an important step in the identification of the "As-Is" operational architecture (OA) and the development of the "To-Be" OA.

3. Narrative

The preferred WBS for documenting the functionality of current system is the one used to design the system. This will provide an exact functionality match between regulatory functional task/subtask and the task the system performs. If an acceptable WBS is not available, use Army Regulations as basis (also, DoDD's and DoDI's) for the particular functional process.

4. Example

a. To identify the functions the mission area is required to perform, look at:

1. AR 10-5, Organizations & Functions, Other AR 10- Series
2. AR 11-3, Department of the Army Functional Reviews results
3. AR 11-40, Functional Area Analysis results.

b. To identify specific task and subtask performed in the mission area look at OMB or DoD Business Reference Models (BRM) or the appropriate Army Regulation:

1. AR 37 series—Financial Management or DFAS 7900.4 Federal Requirements for Financial Management Systems
2. AR700 series—Logistics
3. AR55 series—Transportation

Army Enterprise Integration Oversight Office (AEIOO)
HDQA, C10/G6
www.army.mil/aeioo

LMI
GOVERNMENT CONSULTING
2000 Corporate Ridge
McLean, Virginia 22102
703.917.9800
www.lmi.org
© Copyright 2005, Logistics Management Institute, Version 2, July 2005.